

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-266671

(43)公開日 平成6年(1994)9月22日

(51)Int.Cl.⁵

G 0 6 F 15/00

識別記号

3 3 0 F 7459-5L

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数1 F D (全 7 頁)

(21)出願番号

特願平5-77722

(22)出願日

平成5年(1993)3月11日

(71)出願人 000153465

株式会社日立テレコムテクノロジー

福島県郡山市字船場向94番地

(72)発明者 船場 功

福島県郡山市字船場向94番地 株式会社日

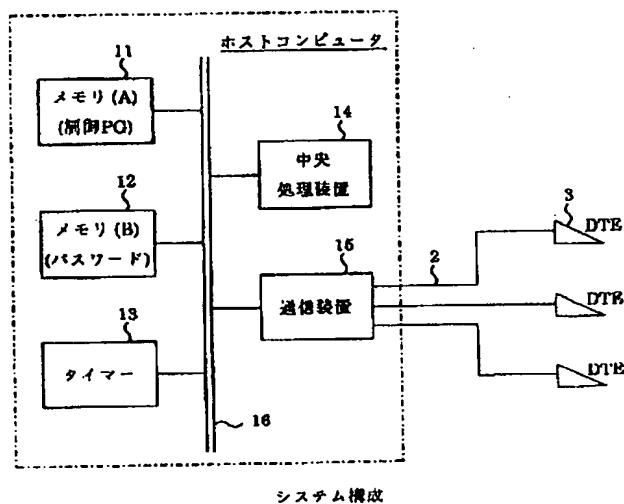
立テレコムテクノロジー内

(54)【発明の名称】 パスワード認識方式

(57)【要約】

【目的】IDコードに対応するパスワードを年月日、時間等により自動的に変更し、セキュリティを向上させる。

【構成】ホストコンピュータ1のメモリ(B)12には、IDコードに対応するパスワードデータを示すテーブルが備えてある。そのテーブルのパスワードデータは月毎、または、年月日、時間毎にパスワードを変更させるためのデータである。そして、端末装置3からIDコードが入力されると、中央処理装置14はタイマー装置13からの時間情報とメモリ(B)12内のテーブルによりカレントパスワードを決定し、端末装置3から入力されるパスワードとカレントパスワードにより、セキュリティチェックを行なう。



【特許請求の範囲】

【請求項1】入力装置と、IDコードに対応するパスワード情報を記憶する記憶装置と、タイマー装置と、これらを制御する制御装置と、を有するパスワード認識方式であって、

上記制御装置は、上記入力装置からIDコードが入力されたとき、上記タイマー装置から得た時間情報と上記記憶装置に記憶されているパスワード情報とに基づいてカレントパスワードを決定し、上記入力装置から入力されたパスワードが上記カレントパスワードと対応した場合に、上記入力装置から入力されたIDコードとパスワードとが対応すると認識することを特徴とするパスワード認識方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、入力されたIDコードと自動的に変更されるパスワードとの対応関係を認識するパスワード認識方式に関する。

【0002】

【従来の技術】従来からキャッシュカードを利用するサービス、パソコン通信におけるネットワークサービス等を受ける場合、IDコードとパスワードとを入力し、その対応関係によりセキュリティチェックを行ないサービスを提供している。このように用いられているパスワードは、IDコードに対応して固定的に設定されており、任意に変更することができなく、変更を要する場合は人為的に行なっている。

【0003】

【発明が解決しようとする課題】上記従来技術は、利用者個人別にパスワードを付与するものであり、あるサービスを受けるためのパスワードを変更する場合、人為的に行なわなければならない。また、他人にパスワードを知られた場合、その他人にそのサービスを受けられてしまう可能性があり、セキュリティに問題があった。

【0004】本発明の目的は、この問題を解決するために、一定期間を経過後、パスワードを自動変更することによって、パスワードを必要とするサービスのセキュリティを高めることにある。

【0005】

【課題を解決するための手段】本発明は、入力装置と、IDコードに対応するパスワード情報を記憶する記憶装置と、タイマー装置と、これらを制御する制御装置とを有するパスワード認識方式であって、上記制御装置は、上記入力装置からIDコードが入力されたとき、上記タイマー装置から得た時間情報と上記記憶装置に記憶されているパスワード情報とに基づいてカレントパスワードを決定し、上記入力装置から入力されたパスワードが上記カレントパスワードと対応した場合に、上記入力装置から入力されたIDコードとパスワードとが対応すると認識することを特徴とする。

【0006】

【作用】上記した構成により、時間によってパスワードが自動的に変更されるので、パスワードを必要とするサービス(ATM、CD、ネットワークサービスなど)において、その安全性を高めることができる。

【0007】

【実施例】以下に本発明の一実施例として、コンピュータネットワークにおいて、本発明のパスワード方式を用いた端末装置からのログインについて具体的に説明する。尚、説明にあたり、入力されたパスワードをインプットパスワード、入力されるべきパスワードをカレントパスワード、データテーブル中にあるパスワード群と、カレントパスワードを求めるための演算式をパスワードデータと、この演算式をパスワード演算式と称して説明する。

【0008】図1は本システムの一構成例を示す図であり、ホストコンピュータ1に通信回線2によって、複数の端末装置3が接続されている。ホストコンピュータ1には、制御プログラム等が格納されているメモリ(A)11と、パスワードデータテーブルを格納しているメモリ(B)12と、タイマー装置13と、端末装置3を接続する通信装置15と、これら全体を制御する中央処理装置14と、が備えられており、それら各装置はバス16で接続されている。

【0009】図2は、パスワードデータテーブルの構成を示す図であり、IDコードに対応してパスワードデータが存在する。IDコード、N001~N004は、1~12月までの月毎のパスワードデータを持っている。またIDコード、N005~S007(例えば、頭のNは、一般ユーザ、Sはスーパーユーザの様にいろいろな特権が与えられている特権ユーザとしている。)は、パスワードデータとしてパスワード演算式を持ち、時間を基にカレントパスワードを生成する。ここで云う時間とは、年/月/日/時/分/秒/曜日/季節などを指すものである。

【0010】以下、本発明の一実施例であるパスワードデータの作成、及び修正について図3に基づいて説明する。

【0011】端末装置3から、スーパーユーザが、IDコード及び、パスワードの設定または変更のコマンド入力により、ホストコンピュータの中央処理装置14は図3に示すフローチャートに基づく制御を実行する。まず、端末装置3からIDコードを入力する(ステップ301)。このIDコードが存在しなければ(ステップ302)、再度IDコードを入力する状態にする(ステップ301)。IDコード入力時に「NEXT」と入力した場合、存在するIDコードの次のIDコードが新規のIDコードとして自動的に指定される。次にパスワード演算を使ってパスワードを作るか、月毎の任意なパスワードを作るか聞いてくるのでどちらかを選択し(ステッ

3

ブ304)、後者ならパスワードの有効な月(例えば、9月なら9)を指定し、さらにその月で使用するパスワードを入力する(ステップ305)。なお、このとき、パスワードの有効文字数以内で、任意の文字や数字をパスワードとして指定できる。そのパスワードが、パスワードの最大文字数を越えるなどして無効な場合は(ステップ306)、再度パスワードを入力する(ステップ305)。有効パスワードなら、パスワードデータテーブルから先に指定したIDコードをサーチし、指定月のパスワードデータとして、先のパスワードを格納する(ステップ307)。新規IDコードなら、ここでテーブル中にIDコードを追加し、同じ様にパスワードを格納する。

【0012】次に、他の月のパスワードも入力するかどうか聞いてくるので、繰り返すかどうか指定する(ステップ308)。ここで、パスワードデータの入力を終了する場合「終了」を選択すると、指定IDコードの1月~12月までのパスワードデータが、端末のディスプレイに表示され、パスワードを確認できる。(ステップ309)。このとき、1月~12月までの全月のパスワードを指定しなかった場合、例えば1月は指定したが、2月、3月は指定しなかった場合、2月、3月の月において1月のパスワードデータが用いられる。即ち、現在の月のパスワードデータが存在しなかった場合は、前の月のパスワードデータがパスワードデータとなって、パスワードデータテーブルに記録される(ステップ309)。

【0013】ステップ304において、パスワード演算を用いる方を選択した場合、パスワード演算式を入力する(ステップ310)。パスワード演算式は、図5に示す関数、算術演算子(+, -, ×, ÷等)、クォーテーションマーク(")で囲んだ文字から成り、これらは「&」によって区切られている。例として、下記の数式1、数式2、及び数式3を挙げる。

【0014】

【数1】

Fa=S\$(1, 1)&D2&D1&S\$(2, 1)&M\$(1, 2)

【0015】

【数2】

Fb="PAS"&D\$(1, 1)&T2+1&M2×3

【0016】

【数3】

Fc=M2&T1&T2&D1&D2&M\$(2, 2)&Y1

【0017】例えば、現在が、1992年9月14日(月)12時07分であると仮定すると、Faは「A14USE」と、Fbは「PASF321」と、Fcは「02141EP2」と、それぞれ定義される。Fbで

4

は加算と乗算を行なっているためカレントパスワードが可変長となっている。除算のときは、小数点以下を切り捨てるようにすると好適となる。なお、このステップ310においては、入力に際し、右辺の演算式のみ入力する。

【0018】このように、パスワード演算式を入力したら、入力した演算式をチェックし(ステップ311)、無効であれば再度入力を促す。有効であれば、対応するIDコードのパスワードデータとして登録する(ステップ312)。そして最後にもう一度パスワードデータ(ここでは演算式)を確認し、IDコードの登録あるいはパスワード変更のモードを終了する。

【0019】以下、図2のパスワードデータテーブルが既に作られたものとして、端末装置からログインする場合の動作を図4に基づいて説明する。

【0020】まず、IDコードを入力する(ステップ401)。入力IDコードよりパスワードデータテーブルをサーチし(ステップ402)、パスワード演算を使っているか調べる(ステップ403)。このとき、入力されたIDコードが存在しない場合、ログイン失敗となる(ステップ409)。パスワード演算を使っていない場合、システム中のタイマー装置13から、月を求め、パスワードデータテーブルからその月に対応するパスワードデータをカレントパスワードとする(ステップ404)。図2では、IDコード、N001~N004にあたる。演算式を使っている場合、即ち、パスワードデータとしてパスワード演算式が存在する場合、この式に基づいてタイマー装置13葉、現在時間のカレントパスワードを求める(ステップ405)。図2では、IDコードN005~S007にあたる。

【0021】次に、端末装置からインプットパスワードを入力する(ステップ406)。カレントパスワードとインプットパスワードを比較し一致すれば(ステップ407)、入力されたIDコードとインプットパスワードが対応したことになりログイン成功となる(ステップ408)。これが一致しなければ、再度インプットパスワードを入力し直し(ステップ406)となるが、3回行っても一致しなければ(ステップ409)、ログイン失敗のルーチン(ステップ410)へ制御を遷移させ、処理を終了する。

【0022】このように、日時、時間等によってパスワードを自動的に変更させると、IDコードとパスワードとの対応関係を複雑にできるので、セキュリティ性が向上する。

【0023】

【発明の効果】以上のように、パスワードが一定期間によって自動変更される為、パスワードを用いるサービスのセキュリティを高めることができる。

【0024】また、パスワード演算を用いた場合、演算式そのものがパスワードの本質であると考え、ある

時点におけるパスワードは一時的なものに過ぎないので、パスワードにロックをかけたと同じ効果を奏することとなる。

【図面の簡単な説明】

【図1】本発明の一実施例を示すシステム構成図である。

【図2】パスワードデータテーブルの構成を示す図である。

【図3】パスワードデータ作成、修正ルーチンを示すフローチャートである。

【図4】ログインルーチンを示すフローチャートである。

【図5】パスワード演算に用いる関数の一例を示す図である。

【符号の説明】

1…ホストコンピュータ

11…メモリ(A)

12…メモリ(B)

13…タイマー装置

14…中央処理装置

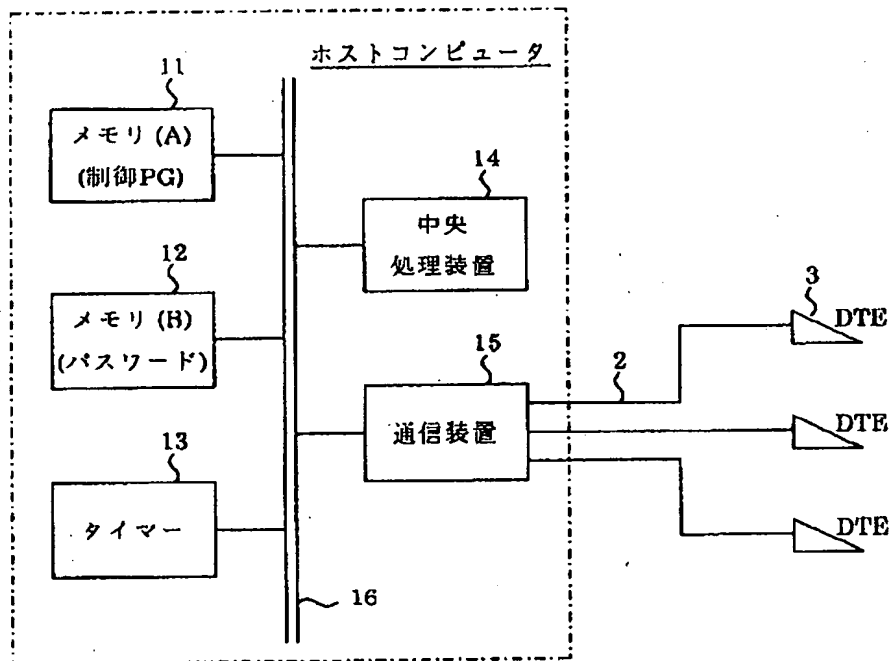
15…通信装置

16…バス

2…通信回線

3…端末装置

【図1】



システム構成

【図2】

ID	パスワード 演算	1月	2月	12月
N001	——	JAN01	FEB02	DEC12
N002	——	AB2100	AB2300	AB2400
N003	——	0116	0216	1216
N004	——	09141970	07291968	BR1SS
N005	Fa	——	——	——
S006	Pb	——	——	——
S007	Fc	——	——	——
.
.
.

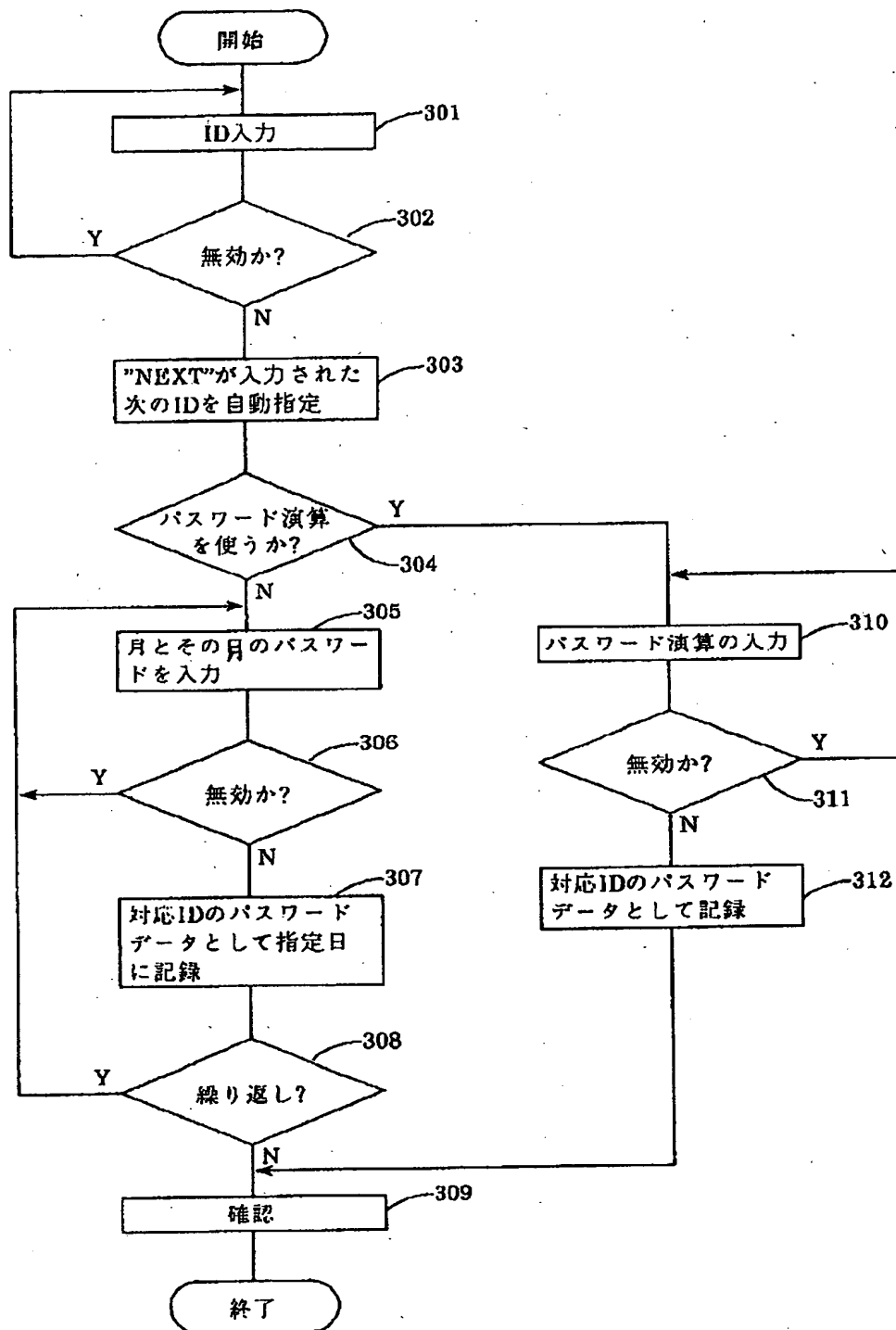
パスワードデータテーブル構成

【図5】

書式	意 味
Yn	西暦による年のn桁目の数字
Mn	月のn桁目の数字
Dn	日のn桁目の数字
Tn	時のn桁目の数字
Mn	分のn桁目の数字
Sn	秒のn桁目の数字
M\$(m,n)	月を英語で表わしたm番目からn文字分の文字列
D\$(m,n)	日を英語で表わしたm番目からn文字分の文字列
S\$(m,n)	季節を英語で表わしたm番目からn文字分の文字列
WK	その月の第何週目かを表わす数字

パスワード演算に用いる関数の一例

【図3】



【図4】

